CLAIMS

1. A method for providing an encrypted transport stream, the method comprising the steps of:

receiving a clear stream, the clear stream including a plurality of programs, each program comprising a plurality of packets each having a packet identifier (PID), wherein at least one of the plurality of packets is designated a critical packet;

scrambling the clear stream according to a first encryption method to provide a first encryption stream;

scrambling the clear stream according to a second encryption method to provide a second encryption stream;

aligning in time the clear stream, the first encryption stream, and the second encryption stream;

passing packets of the clear stream through a multiplexer, wherein when the at least one critical packet is identified in the packets of the clear stream, the critical packet of the clear stream drops and the scrambled critical packets included in the first and second encryption streams pass; and

multiplexing the packets of the clear stream and the critical packets of the first and second encryption streams to provide a partial dual encrypted stream.

2. The method of claim 1, the steps further comprising remapping at least one PID value associated with the second encryption stream, whereby the scrambled packets of the first and second encryption streams each have a differing PID value.

3. The method of claim 1, wherein the aligning step comprises buffering each of the clear stream, the first encryption stream, and the second encryption stream.

4. The method of claim 3, the aligning step comprising the further steps of:

searching the clear stream for a reference packet; and

comparing the reference packet with packets in the first encryption stream and the second encryption stream, wherein the packets associated with the clear stream passes and the packets associated with the first and second encryption streams drop until the packets associated with the first and second encryption stream match the reference packet.

5. The method of claim 1, comprising the further step of demultiplexing each of the clear stream and the first and second encryption streams to provide a plurality of programs.

6. The method of claim 5, wherein a common program demultiplexed from each stream is provided to a common aligner, identifier, and remapper device.

7. A partial dual-encryption device, comprising:

a port for providing a first encrypted stream from a first scrambler;

a port for providing a second encrypted stream from a second scrambler;

an aligner, identifier, and remapper (AIR) device coupled to each scrambler for providing a partial dual-encrypted stream,

wherein a clear stream having at least one critical packet is provided to each scrambler and the AIR device, wherein the AIR device aligns packets of the clear stream, the first encrypted stream, and the second encrypted stream, and wherein, upon identification of the at least one critical packet of the clear stream, provides the partial dual-encrypted stream including non-critical packets of the clear stream, a critical packet of the first encrypted stream, and a remapped critical packet of the second encrypted stream.

8. The partial dual-encryption device of claim 7, the AIR device comprising:

an aligner for aligning the packets associated with the clear stream, the first encrypted stream, and the second encrypted stream;

an identifier for identifying the at least one critical packet; and

a remapper for remapping a packet identifier (PID) value associated with the second encrypted stream,

the aligner comprising:

buffers for buffering the clear stream, the first encrypted stream, and the second encrypted stream; and

a packet comparator for comparing a head packet associated with each stream in a buffer to determine when the buffered streams are aligned and subsequently releasing the streams for further processing.

9. The partial dual-encryption device of claim 8, the AIR device further comprising:

switches responsive to the identifier for allowing one of the packets associated with the clear stream and the packets associated with the first and second encrypted streams to pass through to a multiplexer.

10. The partial dual-encryption device of claim 7, further comprising:

a first demultiplexer coupled to the first scrambler to provide a plurality of first encrypted program streams;

a second demultiplexer coupled to the second scrambler to provide a plurality of second encrypted program streams; and

a third demultiplexer for providing a plurality of clear program streams,

wherein the demultiplexed program streams are provided to the AIR and processed as a common program.

11. The partial dual-encryption device of claim 10, wherein the AIR device includes a plurality of program AIR devices depending upon the number of common programs.

12. The partial dual-encryption device of claim 11, further comprising a common multiplexer for multiplexing the partial dual-encrypted stream from each of the plurality of program AIR devices.

13. The partial dual-encryption device of claim 12, wherein the common multiplexer provides feedback to each of the program AIR devices that indicates availability of bandwidth for when the number of critical packets of the first encrypted stream and the remapped critical packets of the second encrypted stream can be increased.

14. A method for transmitting an encrypted transport stream, the method comprising the steps of:

receiving a clear stream, the clear stream including a plurality of programs, each program comprising a plurality of packets each having a packet identifier (PID), wherein at least one of the plurality of packets is designated a critical packet;

scrambling with a first scrambler the clear stream according to a first encryption method to provide a first encrypted stream;

aligning in time the clear stream and the first encrypted stream;

identifying the at least one critical packet associated with the clear stream, wherein prior to identification, packets associated with the clear stream pass to a multiplexer and encrypted packets associated with the first encrypted stream drop, and wherein subsequent to identification, packets associated with the clear stream pass to a second scrambler and encrypted packets associated with the first encrypted stream pass to the multiplexer, wherein the second scrambler provides a second encrypted stream to the multiplexer; and

multiplexing non-critical packets associated with the clear stream and the encrypted critical packets associated with the first and second encrypted streams to provide a partial dual-encrypted stream.

15. The method of claim 1, the steps further comprising remapping the second encrypted stream to a new PID value.

16. A partial dual-encryption device, comprising:

a port for providing a first encrypted stream from a first scrambler;

an aligner, identifier, and remapper (AIR) device coupled to the scrambler for providing a partial dual-encrypted stream,

wherein a clear stream having at least one critical packet is provided to the scrambler and the AIR device, wherein the AIR device aligns packets of the clear stream and the first encrypted stream, and identifies the at least one critical packet associated with the clear stream, wherein, upon identification of the at least one critical packet, provides the at least one critical packet to a second scrambler, the second scrambler to provide a second encrypted stream, and wherein the AIR device provides the partial dual-encrypted stream including non-critical packets associated with the clear stream and dually-encrypted critical packets associated with the first and second encrypted streams.

17. The partial dual-encryption device of claim 16, the AIR device comprising:

an aligner for aligning the packets associated with the clear stream and the first encrypted stream;

an identifier for identifying the a critical packet associated with the clear stream; and

a first switch responsive to the identifier for providing one of the non-critical packets associated with the clear stream to a multiplexer and the critical packet associated with the clear stream to a second scrambler;

a second switch responsive to the identifier, wherein upon identification of the critical packet, the second switch for providing a first encrypted critical packet of the first encrypted stream to the multiplexer;

the second scrambler coupled to the first switch for receiving the critical packet associated with the clear stream and providing a second encrypted critical packet; and

a remapper for remapping the second encrypted packet to provide a remapped encrypted critical packet.

18. The partial dual-encryption device of claim 17, the AIR device comprising:

a first demultiplexer coupled to the first scrambler to provide a plurality of first encrypted program streams; and

a second demultiplexer for providing a plurality of clear program streams,

wherein the demultiplexed program streams are provided to the AIR device and processed according to a common program stream.

19. The partial dual-encryption device of claim 18, wherein the AIR device includes a plurality of program AIR devices depending upon the number of common program streams.

20. The partial dual-encryption device of claim 19, further comprising a common multiplexer for multiplexing the partial dual-encrypted stream from each of the plurality of program AIR devices, wherein the common multiplexer provides feedback to each of the program AIR devices that indicates availability of bandwidth for when the number of critical packets of the first encrypted stream and the remapped encrypted critical packets of the second encrypted stream can be increased.